AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Michael McCullagh, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations (HSI). HSI is a directorate within Immigration and Customs Enforcement (ICE). ICE is a subordinate component of the Department of Homeland Security (DHS), a department in the executive branch of the United States of America. ICE is the successor to many of the law enforcement powers of the former Immigration and Naturalization Service and the former U.S. Customs Service. I have been a Special Agent since July 2002. Upon graduating from the Federal Law Enforcement Training Center, I was assigned as a Special Agent for the U.S. Customs Service in the Special Agent in Charge (SAC) New York Office in New York City. In October 2007, I transferred to the Burlington, Vermont Resident Agent in Charge Office, where I presently work. I hold a Bachelor of Science degree in Business Administration from Saint Michael's College. I have been a computer forensic agent (CFA) for my agency since 2006, and have participated in many child pornography and child exploitation investigations. Prior to my employment with HSI, I was a police officer with the Winooski, Vermont Police Department. Throughout my career, I have gained experience, through training and everyday work, in investigating violations relating to child exploitation and child pornography, including

the receipt, transportation, possession, and distribution of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States. During such investigations, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous child pornography investigations and am very familiar with the tactics used by child pornography offenders who collect and distribute child pornographic material.

3. I make this affidavit in support of an application for a search warrant for the entire premises, including the residential dwelling and any shed or free-standing structure located at the premises, located at 21 Garden Street, Bennington, VT 05201, the body of any person on the Subject Premises at the time of the search or who comes onto the Subject Premises during the search, and any vehicle found on the Subject Premises at the time of the search or which comes onto the Subject Premises during the search (collectively referred to as the "Subject Premises"). I have probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252 (advertising, receipt, and distribution of possession of child pornography) are located within the Subject Premises. I submit this application and affidavit in support of a search warrant authorizing a search of the entire Subject Premises, as further described and depicted in Attachment A, which is incorporated here by reference.

4. I request authority to search the entire Subject Premises, and any computer and computer media located there, for items specified in Attachment B (which is incorporated by reference) which may be found, and to seize all items listed in Attachment B as contraband and evidence, fruits, and instrumentalities of a crime.

5. The statements contained in this affidavit are based on information provided by HSI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by HSI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with HSI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation.

DEFINITIONS

6. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage

functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(1).

c. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

e. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be

translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

j. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

m. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS, DIGITAL MEDIA, & CHILD PORNOGRAPHY

7. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, computers, computer technology, other digital electronic storage devices, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

8. Computers and other digital electronic media basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

9. Child pornography offenders can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, electronic devices such as Apple iPhones, Apple iPads, e-readers, and tablets now function essentially as computers with the same abilities to store images in digital form.

11. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! Inc., and Google Gmail, among others. The online service(s) allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account(s) from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer or electronic media. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As with most digital technology, communications made from a computer or other electronic device are often saved or stored on that computer or device. Storing this information can be intentional, for example, by saving an email as a file on the computer

or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

13. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space. These types of deleted files can remain in this free or slack space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted

data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed but more on a particular user's operating system, storage capacity, and computer habits.

14. Because the distribution of child pornography is illegal, child pornography is not readily available through legitimate domestic businesses. However, in contrast, child pornography is widely available via computer or other digital electronic media from individuals who trade such material on the Internet. An individual can use the computer or other digital electronic media in the privacy of his/her own home or office to locate and interact with other individuals offering or seeking such materials. Moreover, an individual can do so without revealing his/her true identity. The use of computers and other digital electronic media devices provide individuals interested in child pornography or obscene images with a convenient method of storing, organizing, and accessing their collection and information concerning other who collect, trade, or distribute such materials.

15. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer

related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following three reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data.

c. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

16. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit. In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media).

17. Furthermore, because there is probable cause to believe that the computer and its storage devices, and other digital electronic media are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

BACKGROUND OF INVESTIGATION

18. In August 2016, officers with the New York City Police Department (NYPD) arrested an individual for a violation of New York State Penal Laws 263.15 and 263.16, promotion and possession of a sexual performance by a child. On August 26, 2016, NYPD officers provided information to Homeland Security Investigations - New York, Child Exploitation Investigations Unit, about multiple email accounts used by that individual to trade child exploitative material.

19. The individual arrested provided NYPD officers with written consent and the passwords needed to access email accounts which he had used to engage in the trading of child exploitative material. As a result of this, multiple email accounts were found to have traded child pornography with this individual.

20. One of the email addresses identified as having traded child exploitative material with the individual arrested in New York was: electronic mail account theandreahenderson5@gmail.com ("the Subject Email Account"). On August 26, 2016, HSI agents in New York sent a summons to Google requesting the following information associated with the Subject Email Account: all records regarding the identity of the customer to include, but not limited to, registrant name, address, associated email

addresses, all MAC addresses, telephone number, status of account, available IP history, length of service, and date account was opened. The response from Google included two IP addresses which were associated with a total of eight log-ins for the account. Two of the log-ins were as follows: 2601:181:200:3f23:f556:d087:ceae:f4fe on 07/10/16 at 01:37:41 UTC, and 2601:181:200:3f23:221:e9ff:feda:1781 on 07/01/2016 at 12:47:27 UTC. HSI agents in New York determined that the Internet Service Provider (ISP) for these IP addresses was Comcast.

a. I confirmed that the ISP for the IP addresses was Comcast using a geo-lookup website which allowed for identification of the geographic location of IP addresses, including latitude, longitude, city, region, and country.

b. On November 8, 2016, I spoke with Jonathan Ma, a Custodian of Records from Google. Mr. Ma indicated that the IP login history provided to the HSI New York Agent was an accurate record of the IP login history on file for this email account through August 26, 2016, which was the date of the summons. This record showed the last login for this gmail account as July 10, 2016. Mr. Ma explained that it is possible on a variety of electronic devices, such as an Android phone, for the service to just stay logged in; therefore, account activity may occur after that login date without Google recording any additional IP history.

21. On September 21, 2016, HSI NY Agents sent a summons to Comcast requesting all records regarding the identity of the customer to include, but not limited to, registrant name, address, associated email addresses, all MAC addresses, telephone

number, status of account, available IP history, length of service, and date account was opened concerning the account using IP addresses 2601:181:200:3f23:f556:d087:ceae:f4fe on 07/10/16 at 01:37:41 UTC and 2601:181:200:3f23:221:e9ff:feda:1781 on 07/01/16 at 12:47:27 UTC. On September 22, 2016, Comcast provided a response which identified the subscriber of the IP addresses associated with the Subject Email Account as Donald Hammalian, 21 Garden Lane in Bennington, Vermont 05201 (the Subject Premises).

PROBABLE CAUSE

22. On September 30, 2016, HSI SA Caitlin Moynihan was contacted by HSI SA Patricia Pliva, who advised that an email address being used to trade child exploitative material had resolved back to an address located in Bennington, Vermont. Agent Pliva advised that she had copies of an email exchange, including Google Drive links and the suspected child pornography files, that the target in Vermont had emailed to the individual arrested in New York City.

23. The lead information packet received by SA Pliva included the following: a screenshot of a Google drive file named "novosvideos.zip" which included the names of eight video files (at the top of this screenshot, in the address bar of the window, the following is displayed: https://drive.google.com/file/d/0B-yuvwCd7yruVUZsdUU5X2IxWWM/view); a screenshot of the folder "novosvideos" which displayed the eight files names and a still image associated with each file; a zip file named "hot vids.zip"; a file named "novosvideos.zip"; a folder titled "hot vids" which

contained four movie files containing suspected child pornography and a folder titled "novosvideos" which contained eight movie files, some of which contained suspected child pornography files.) Additionally, SA Pliva provided a screenshot of an email titled "Re: Some to start..." Directly below the subject line of this email it says "From: Andrea Henderson". This is an email which had been received by the individual who was arrested in New York City. The original email was sent on July 22, 2016 from the Subject Email Address. In the body of the email are two links: https://drive.google.com/file/d/0B-yuvwCd7yruVUZsdUU5X2IxWWM/view, and https://drive.google.com/file/d/0B-yuvwCd7yruNWsyelV6N2RIdW8/view. There is no response from the individual in New York City and on July 28, 2016 at 7:07 am, the Subject Email Account sent an additional email message which stated, "Guess you don't want to trade then..."

24. I have viewed the eight files and based on my training and experience, I believe that seven of the files contain child pornography; that is, contain images of a child engaged in sexually explicit conduct. Two of the video files of child pornography are described below:

a. Filename: tara 11yr – 2010 dad.wmv – The video file is approximately 5 minutes and 1 second in length. The video begins with a nude pubescent female child performing oral sex on an adult male. At approximately 1 minute and 30 seconds in the video, the pubescent female child is on top of the adult male and they are engaging in vaginal intercourse. At approximately 3 minutes and 00 seconds in the video, the pubescent female child is again performing oral sex on the adult male. At approximately 3 minutes and 40 seconds in the video, the pubescent female child squats over the adult male and he inserts his penis into her vagina. The pubescent female child has minimal breast

development and no visible pubic hair.

b. Filename: VID-20160219-WA0081.mp4 – The video file is approximately 1 minute and 31 seconds in length. The video depicts a prepubescent female child and an adult male. The prepubescent female child is kneeling on the bed and the adult male is standing on the ground behind her. The adult male inserts his penis into the prepubescent female child; however, it is unknown whether it was inserted into her vagina or her anus. The prepubescent female child can be heard whimpering in pain. The adult male continues to thrust his penis into the prepubescent female child. At one point the adult male can be heard saying "put your chest down for me, get down." At approximately 1 minute and 10 seconds in the video, the adult male says "I'm gonna cum in your butt…(inaudible)" The adult male then appears to ejaculate inside of the prepubescent female child. The prepubescent female child does not appear to have any breast development. Her genitals are not visible to the camera, so it is unknown if there is any visible pubic hair.

25. Research was conducted into the subscriber, Donald Hammalian which is the name on the account information provided by Comcast, as follows:

a. A request was sent to the Vermont Fusion Center for information on Donald Hammalian. The Vermont Intelligence Center (also known as the Fusion Center) provides accurate and timely strategic intelligence products to assist agencies with criminal cases, which includes but is not limited to background intelligence on persons suspected of criminal activity, timelines, and link charts to assist in organizing a case. The Fusion Center response indicated that Donald Hammalian, born in 1974, resided at 21 Garden Lane, Bennington, Vermont 05201. The response also indicated that Donald Hammalian was a registered sex offender under the supervision of Vermont U.S. Probation Officer (USPO) Doug Cowher.

a. I have reviewed a Judgment in case number 6:09-CR-86-ORL-35KRS from the Middle District of Florida. The Judgment indicates that Hammalian was sentenced on January 6, 2010, to serve 48 months imprisonment following his guilty plea to one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B), (b)(2). The Judgment also indicated that Hammalian was to be placed on supervised release for a term of 20 years upon his release from imprisonment.

26. I contacted USPO Cowher to speak with him regarding Hammalian. USPO Cowher advised that Hammalian earns a living by running an eBay business where he sells other people's property for a fee. USPO Cowher warned that Hammalian has video surveillance cameras both inside and outside of his residence, to include on his driveway. USPO Cowher recommended that investigators not drive onto Garden Lane, as Hammalian's cameras will capture their vehicle. USPO Cowher indicated that 21 Garden Lane can be seen from Dewey Street, and described the Subject Premises as being a Cape Cod style house, green in color, with a two car attached garage. USPO Cowher also advised there is a shed behind the residence which also contains video surveillance cameras inside of it; he further advised that Hammalian drives a light blue pickup truck.

27. On October 18, 2016, SA Caitlin Moynihan and I conducted surveillance of the Subject Premise from Dewey Street, which is the street the front yard of the Subject Premises borders. Garden Lane can be described as a very small road, which appears to connect the driveways of the three houses on it. While driving past Garden Lane, SA Moynihan and I observed a pickup truck, blue in color, turn onto Dewey Street from

Garden Lane. I noticed the eBay logo on a sticker affixed to the side of the truck. The truck matched the description provided by USPO Cowher. The Subject Premises were observed and photographed from Dewey Street due to presence of video surveillance cameras being used by Hammalian, and there were some bushes and trees which obscured some of the view of the residence.

28. A record check conducted though the Vermont Department of Motor Vehicles revealed that Hammalian has the following vehicle registered to him, a 1996 Ford truck, blue in color, bearing Vermont registration 217A626.

29. I have viewed the residential dwelling located at the Subject Premises and describe it as follows: a multiple story, Cape Cod style house, located at 21 Garden Lane, Bennington, Vermont. It has green siding and a dark grey roof. The house is broken into three attached sections which will be described as viewed from Dewey Street: The center section appears to be the main living section of the residence and is taller than the other two sections. On the left side of the residence there is a two car attached garage, and the right side of the house appears to be additional living space. A white storm door can be seen on the right side of the residence. Due to the limited viewpoint I had of the residential dwelling, I showed the pictures I took of it to USPO Cowher, and he confirmed it was the residence of Donald Hammalian, located at 21 Garden Lane, Bennington, Vermont. I have included as part of Attachment A accurate photographs of the residential dwelling located at the Subject Premises.

SEARCH METHODOLOGY TO BE EMPLOYED

30. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;

b. Examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. Surveying various file directories and the individual files they contain;

e. Opening files in order to determine their contents;

f. Scanning storage areas;

g. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

h. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

31. Based on the foregoing, I believe that there is probable cause to believe that (1) an individual at the Subject Premises used a computer or other digital device which was connected to the Internet from the Subject Premises to violate Title 18, United States Code, Sections 2251 and 2252, which make it a federal crime for any person to knowingly receive, distribute, advertise, or possess child pornography; and (2) the fruits, evidence, contraband, and instrumentalities of these offenses, described in Attachment B are located at the Subject Premises.

32. Based on the foregoing, I respectfully request that this Court issue a warrant to search the Subject Premises, which is more particularly described in Attachment A, and authorizing the seizure of the items described in Attachment B.

11/9/2016

MICHAEL MCCULLAGH
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on 9th November 2016.

HONORABLE JOHN M. CONROY
UNITED STATES MAGISTRATE JUDGE